DATA TRANSMISSION METHOD

Patent Number: JP4360438
Publication date: 1992-12-14
Inventor(s): MATSUTANI KIYOSHI
Applicant(s):: MITSUBISHI ELECTRIC CORP
Requested Patent: JP4360438
Application Number: JP19910136504 19910607
Priority Number(s):
IPC Classification: H04L9/00 ; H04L9/10 ; H04L9/12 ; G11B20/10
EC Classification:
Equivalents:

Abstract

PURPOSE:To obtain the data transmission method in which decoding is difficult when a personal data or a data with high confidentiality is sent.
CONSTITUTION:Data generated by a pseudo random data generating section 1 based on a password and a service ID or the like in a data to be sent are subject to addition processing in an exclusive OR circuit 14, coded in an error correction coder 3 and data arrangement is rearranged in an interleave section 4. A formatter 5 adds a synchronizing signal and information such as address information, the result is outputted according to a transmission signal format, modulated by a modulation section 6, the personal ID and the password are collated at line connection and the result is sent to a destination designated by an address. The address includes personal ID information and the relevant password and service ID are managed by a personal identification information management section 2 and used for generating a pseudo random data at a receiver side.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平4－360438

(43)公開日　平成４年(1992)12月14日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/00				
9/10				
9/12				
Ｇ１１Ｂ　20/10		Ｈ　7923－5D		
		7117－5K	Ｈ０４Ｌ　9／00	Ｚ

審査請求　未請求　請求項の数４(全　７　頁)　最終頁に続く

(21)出願番号　特願平3－136504

(22)出願日　平成３年(1991)６月７日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　松谷　清志
長岡京市馬場図所１番地　三菱電機株式会社電子商品開発研究所内

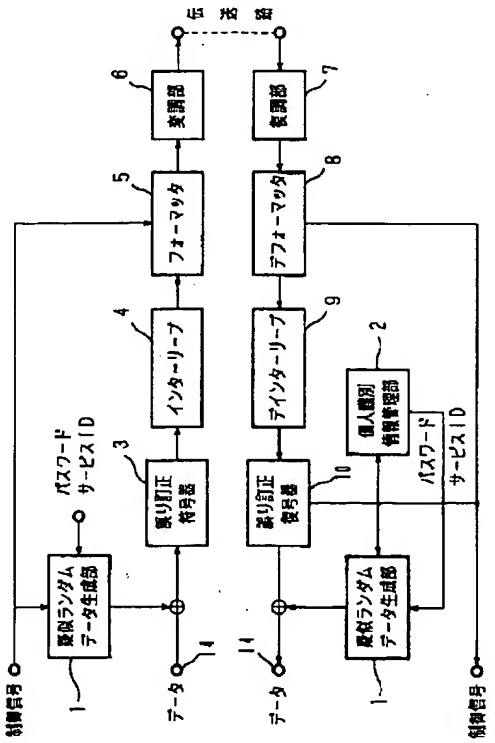
(74)代理人　弁理士　高田　守　(外１名)

(54)【発明の名称】　データ伝送方法

(57)【要約】

【目的】　個人に関するデータや、機密性の高いデータを伝送する場合に、解読困難なデータ伝送方法を提供することを目的とする。

【構成】　伝送されるデータに、パスワードやサービスＩＤ等を基に、疑似ランダムデータ生成部１で生成されたデータを排他的論理和回路１４で加算処理の後、誤り訂正符号器３で符号化が行われ、インターリーブ部４でデータ配列の並べ替えが行われる。フォーマッタ５で同期信号や、アドレス情報等の情報が付加され、伝送信号ホーマットに従って出力、変調部６で変調され回線接続時に個人ＩＤやパスワードを入力照合した後アドレスに指定された宛先へ送付される。このアドレスには個人ＩＤ情報が含まれており、これと対応したパスワードやサービスＩＤは、個人識別情報管理部２で管理され、受信側での疑似ランダムデータ生成に用いられる。



1

【特許請求の範囲】

【請求項１】　双方向データ伝送を行う場合に、個人又は世帯、あるいは法人毎に付与された識別信号と共にデータが伝送され、該データ部分に対しては、該伝送データ中に含まれない、該個人又は世帯、あるいは法人が相互に、もしくはセンターシステムに申請登録した暗唱番号を基に生成した疑似ランダムデータでスクランブルをかけて送信し、受信側で解除することを特徴とするデータ伝送方法。

【請求項２】　上記疑似ランダムデータは、該伝送データ中に含まれる制御信号に基づき、又は一定データ長毎に定期的に更新されることを特徴とする請求項１記載のデータ伝送方法。

【請求項３】　双方向データ伝送を行う場合に、個人又は世帯、あるいは法人毎に付与された識別信号（以下、個人ＩＤという。）と共にデータが伝送され、該データ部分に対しては、該伝送データ中に含まれない、該個人又は世帯、あるいは法人が相互に、もしくはセンサーシステムに申請登録した暗唱番号（以下、パスワードという。）と、該個人又は世帯、あるいは法人に対して相互に、もしくはセンターシステムに認可登録された複数種類の情報提供や便宜供与の内容を示す識別信号（以下、サービスＩＤという。）を基に生成した疑似ランダムデータでスクランブルをかけて送信し、受信側で解除することを特徴とするデータ伝送方法。

【請求項４】　上記疑似ランダムデータは、該伝送データ中に含まれる制御信号に基づき、又は一定データ長毎に定期的に更新されることを特徴とする請求項３記載のデータ伝送方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】個人に関するデータや機密性の高いデータの伝送に関するものである。

【０００２】

【従来の技術】図４はディジタルパケット通信に用いられている信号の一例を示す伝送信号フォーマット図、図５は従来のデータ伝送方法の一例を示すブロック図であり、図において１は疑似ランダムデータ生成部、３は誤り訂正符号器、４はインターリーブ部、５はフォーマッタ、６は変調部、７は復調部、８はデフォーマッタ、９はデインターリーブ部、１０は誤り訂正復号器、図６は従来の疑似ランダムデータ生成部の一例を示す回路構成図であり、図において１３はシフトレジスタ、１４は排他的論理和回路、１５はデータ入力端子、１６はビットシフトクロック入力端子、１７はデータロード信号入力端子、１８はスイッチ、１９はキーデータ入力部、２０はデータ変換ＲＯＭ、図７は従来の疑似ランダムデータ生成部の他の一例を示す回路構成図、図８は従来のデータ伝送方法に用いられている信号の一例を示す伝送信号フォーマット図、図９は従来のデータ伝送方法に用いられている信号の他の一例を示す伝送信号フォーマット図である。

2

【０００３】次に図について説明する。まず、公衆電話回線や専用データ回線を使用したデータ通信においては、回線接続時に個人ＩＤやパスワードを入力照合し、適合した場合のみ接続するように機密保護されており、データは図４に示したようなＣＣＩＴＴ勧告Ｘ．２５に準拠した伝送信号フォーマットで、アドレスに指定された宛先へ送出されるが、データそのものは他の加入ユーザも利用可能な形態で伝送される。

【０００４】次にデータそのものに何等かの保護がなされている例について説明する。送信側では伝送されるデータに、疑似ランダムデータ生成部１で生成されたデータを排他的論理和回路１４で加算処理した後、受信側でのデータ復元の際に重要となる、疑似ランダムデータ生成に用いられたキーデータと共に誤り訂正符号器３で符号化が行われ、インターリーブ部４でデータ配列の並べ替えが行われる。このデータに、フォーマッタ５で同期信号や識別信号、アドレス情報等のヘッダや、受信側でのデータ復元の際に必要となる情報が付加され、伝送信号フォーマットに従って出力されて、変調部６で変調され送出される。

【０００５】受信側では、伝送されたデータを復調部７で復調した後、デフォーマッタ８でヘッダやデータ復元に必要な情報が除去され、デインターリーブ部９で元のデータ配列に戻される。このデータに対して誤り訂正復号器１０で誤り訂正が行われ、信頼性の高い、疑似ランダムデータ生成に用いられたキーデータに基づき、疑似ランダムデータ生成部１で生成したデータを排他的論理和回路１４で加算処理することにより、元のデータが復元される。

【０００６】この疑似ランダムデータ生成部１の内部回路構成は、図６や図７に示したようになっており、キーデータ入力部１９に入力されたｎビットのキーデータがデータロード信号入力端子１７に入力された信号タイミングでシフトレジスタ１３にロードされ、ビットシフトクロック入力端子１６に入力されたクロックでシフトする。（ｎ：自然数）このシフトレジスタの所定のビット間で排他的論理和回路１４で加算処理が行われて順次入力され、図６のように任意の１ビット情報がデータ交換ＲＯＭ２０で変換され、シリアル出力された情報と、あるいは図７のように特定のビット情報とデータ入力端子１５に入力された伝送されるべきデータのシリアル入力が排他的論理和回路１４でビット毎に加算処理される。（ｉ：自然数）この加算されたデータと、加算されないデータがデータ内容によってスイッチ１８で切り換えられながら出力される。

【０００７】疑似ランダムデータ生成に用いられるキーデータは、昭和６３年度の放送衛星によるテレビジョン放送における有料方式に関する技術的条件についての電

3

気通信技術審議会答申によれば、図８のような伝送信号フォーマットにおいて、固有データの中の番組情報に含まれ、その更新用のデータロード信号は、制御符号の中に含まれている。また、ＶＨＳ方式ビデオテープレコーダのディジタル音声記録においては、図９のような伝送信号フォーマットにおいて、スクランブルのかからないアドレス情報部分のデータが用いられ、その更新はこのデータブロック単位で行われる。

【０００８】

【発明が解決しようとする課題】従来のデータ伝送方法は以上のように構成されており、パスワードが設定されていてもデータ回線接続時のチェックが済めば、データ伝送中の機密保護に用いられることはなく、また、データ伝送中の機密保護のため、データにスクランブルがかけられる場合でも、スクランブルをかけるのに用いられる疑似ランダムデータそのものは定期的に異なったパターンに変化するが、疑似ランダムデータ生成の制御情報がすべて伝送データ中に含まれているため、伝送信号フォーマットに対応した機器さえあれば、他の加入ユーザにもスクランブルを容易に解除でき、盗聴の可能性が高いという問題点があった。

【０００９】本発明は、以上のような問題点を解消するためになされたもので、個人に関するデータや機密性の高いデータを伝送する場合に、解読困難なデータ伝送方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明に係るデータ伝送方法は、個人又は世帯、あるいは法人毎に付与された識別信号と共にデータが伝送され、該データ部分に対しては、該伝送データ中に含まれない、該個人又は世帯、あるいは法人が相互に、もしくはセンターシステムに申請登録した暗唱番号を基に生成した疑似ランダムデータでスクランブルをかけて送信し、受信側で解除するようにしたものである。さらに該伝送データ中に含まれる制御信号に基づき、又は一定データ長毎に定期的に更新されるようにしたものである。

【００１１】また、個人又は世帯、あるいは法人毎に付与された識別信号と共にデータが伝送され、該データ部分に対しては、該伝送データ中に含まれない、該個人又は世帯、あるいは法人が相互に、もしくはセンサーシステムに申請登録した暗唱番号と、該個人又は世帯、あるいは法人に対して相互に、もしくはセンターシステムに認可登録された複数種類の情報提供や便宜供与の内容を示す識別信号を基に生成した疑似ランダムデータでスクランブルをかけて送信し、受信側で解除するようにしたものである。さらに該伝送データ中に含まれる制御信号に基づき、又は一定データ長毎に定期的に更新されるようにしたものである。

【００１２】

【作用】本発明におけるデータ伝送方法は、伝送データ

4

中に含まれない個別信号を基に生成した疑似ランダムデータでスクランブルをかけているため、個別信号情報を知り得ない限り、スクランブルを解除することは困難である。

【００１３】

【実施例】

実施例１．図１は本発明のデータ伝送方法の一実施例を示すブロック図であり、図において１は疑似ランダムデータ生成部、２は個人識別情報管理部、３は誤り訂正符号器、４はインターリーブ部、５はフォーマッタ、６は変調部、７は復調部、８はデフォーマッタ、９はデインターリーブ部、１０は誤り訂正復号器、図２は本発明の疑似ランダムデータ生成部の一実施例を示す回路構成図であり、図において１１はパスワード入力部、１２はサービスＩＤ入力部、１３はシフトレジスタ、１４は排他的論理和回路、１５はデータ入力端子、１６はビットシフトクロック入力端子、１７はデータロード信号入力端子、１８はスイッチ、１９はキーデータ入力部、２０はデータ変換ＲＯＭ、図３は本発明の疑似ランダムデータ生成部の他の実施例を示す回路構成図、図４はディジタルパケット通信に用いられる信号の一例を示す伝送信号フォーマット図である。

【００１４】次に図について説明する。送信側では、伝送されるデータに、パスワードやサービスＩＤ、キーデータ等を基に、疑似ランダムデータ生成部１で生成されたデータを排他的論理和回路１４で加算処理した後、受信側でのデータ復元の際に重要となる、疑似ランダムデータ生成に用いられたキーデータと共に誤り訂正符号器３で符号化が行われ、インターリーブ部４でデータ配列の並べ替えが行われる。このデータに、フォーマッタ５で同期信号や識別信号、アドレス情報等のヘッダや、受信側でのデータ復元の際に必要となる、パスワードやサービスＩＤ以外の情報が付加され、伝送信号フォーマットに従って出力されて、変調部６で変調され送出される。

【００１５】公衆電話回線や専用データ回線を使用したデータ通信においては、回線接続時に個人ＩＤやパスワードを入力照合し、適合した場合のみ接続するように機密保護されており、データは図４に示したような伝送信号フォーマットで、アドレスに指定された宛先へ伝送される。このアドレスには個人ＩＤ情報が含まれており、この個人ＩＤと対応したパスワードやサービスＩＤは、個人識別情報管理部２で管理されている。

【００１６】受信側では、伝送されたデータを復調部７で復調した後、デフォーマッタ８でヘッダやデータ復元に必要な情報が除去され、デインターリーブ部９で元のデータ配列に戻される。このデータに対して誤り訂正復号器１０で誤り訂正が行われ、信頼性の高い、疑似ランダムデータ生成に用いられたキーデータと、上記個人識別情報管理部２から出力されたパスワードやサービスＩ

Ｄに基づき、疑似ランダムデータ生成部１で生成したデータを排他的論理和回路１４で加算処理することにより、元のデータが復元される。

【００１７】この疑似ランダムデータ生成部１の内部回路構成は、図６や図７に示したようになっており、パスワード入力部１１に入力された１ビットのパスワードと、サービスＩＤ入力部１２に入力されたｍビットのサービスＩＤと、キーデータ入力部１９に入力されたｎビットのキーデータがデータロード信号入力端子１７に入力された信号タイミングで各々シフトレジスタ１３にロードされ、ビットシフトクロック入力端子１６に入力されたクロックでシフトする。（１，ｍ：自然数）このシフトレジスタの所定のビット間で排他的論理和回路１４で加算処理が行われて順次入力され、図６のように任意の１ビット情報がデータ変換ＲＯＭ２０で変換され、シリアル出力された情報と、あるいは図７のように特定のビット情報とデータ入力端子１５に入力された伝送されるべきデータのシリアル入力が排他的論理和回路１４でビット毎に加算処理される。この加算されたデータと、加算されないデータがデータ内容によってスイッチ１８で切り換えられながら出力される。

【００１８】疑似ランダムデータ生成に用いられるキーデータは、伝送信号フォーマットの中に含まれ、そのキーデータ更新は一定データ長毎に行われるか、更新用のデータロード信号も伝送信号フォーマットの中に含まれている。契約時のパスワードやサービスＩＤの初期値は、他の情報伝達手段に依り提供されるが、その後のパスワードやサービスＩＤの変更や更新情報の伝達は、すべて本データ伝送方法の中で可能であり、該変更や更新情報が伝達されたデータ伝送の回線切断後、次回の回線接続時から適用する。

【００１９】実施例２．尚、上記実施例ではデータに誤り訂正の符号化と復号化、インターリーブとデインターリーブ、変調と復調を行っているが、いずれの処理も行っても行わなくてもよく、その順序も問わないし、その処理方式も任意でよい。

【００２０】実施例３．また、疑似ランダムデータの加算は誤り訂正の符号化の前、復号化の後になっているが、特に限定するものではなく、符号化の後、復号化の前でもよく、インターリーブの後、デインターリーブの前でもよいし、フォーマッタの後、デフォーマッタの前でもよい。

【００２１】実施例４．さらに、パスワードやサービスＩＤ、キーデータ等のビット数は任意でよく、定期的に更新してもしなくてもよいが、定期的に更新する場合は、更新期間内に伝送されるデータ数よりも２（１＋ｍ＋ｎ）が大きくなるように、１，ｍ，ｎを選ぶのが望ましい。また、シフトレジスタのビット間加算位置やデータとの加算用抽出ビット位置も任意でよい。

【００２２】実施例５．また、伝送信号フォーマット

も、伝送先が特定できるアドレス情報が含まれていれば任意でよく、個人ＩＤ以外の同種の識別信号で代用して構わない。

【００２３】実施例６．さらに、個人ＩＤ等のアドレス情報や、疑似ランダムデータ生成に用いられるキーデータ、あるいは受信側でのデータ復元の際に重要となる情報等は、誤り訂正符号の中に含めることが望ましいが、含めなくてもよい。

【００２４】

【発明の効果】本発明におけるデータ伝送方法は、伝送データ中に含まれない個別信号を基に生成した疑似ランダムデータでスクランブルをかけているため、個別信号情報を知り得ない限り、スクランブルを解除することは困難である。従って、伝送信号フォーマットに対応した機器により、伝送データが傍聴されても、他の加入ユーザにスクランブルを解除することはできないという効果がある。

【００２５】また、個人ＩＤ等のアドレス情報や、疑似ランダムデータ生成に用いられるキーデータ、あるいは受信側でのデータ復元の際に重要となる情報等を誤り訂正符号の中に含めることにより、データ信頼性と復元確率を高める効果がある。

【図面の簡単な説明】

【図１】本発明のデータ伝送方法の一実施例を示すブロック図である。

【図２】本発明の疑似ランダムデータ生成部の一実施例を示す回路構成図である。

【図３】本発明の疑似ランダムデータ生成部の他の実施例を示す回路構成図である。

【図４】ディジタルパケット通信に用いられる信号の一例を示す伝送信号フォーマット図である。

【図５】従来のデータ伝送方法の一例を示すブロック図である。

【図６】従来の疑似ランダムデータ生成部の一例を示す回路構成図である。

【図７】従来の疑似ランダムデータ生成部の他の一例を示す回路構成図である。

【図８】従来のデータ伝送方法に用いられている信号の一例を示す伝送信号フォーマット図である。

【図９】従来のデータ伝送方法に用いられている信号の他の一例を示す伝送信号フォーマット図である。

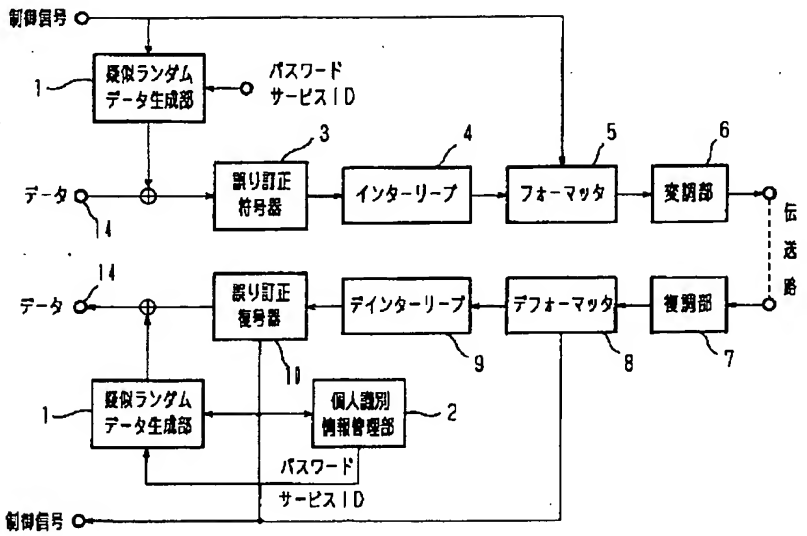
【符号の説明】

１　疑似ランダムデータ生成部
２　個人識別情報管理部
３　誤り訂正符号器
５　フォーマッタ
８　デフォーマッタ
１０　誤り訂正復号器
１１　パスワード入力部
１２　サービスＩＤ入力部

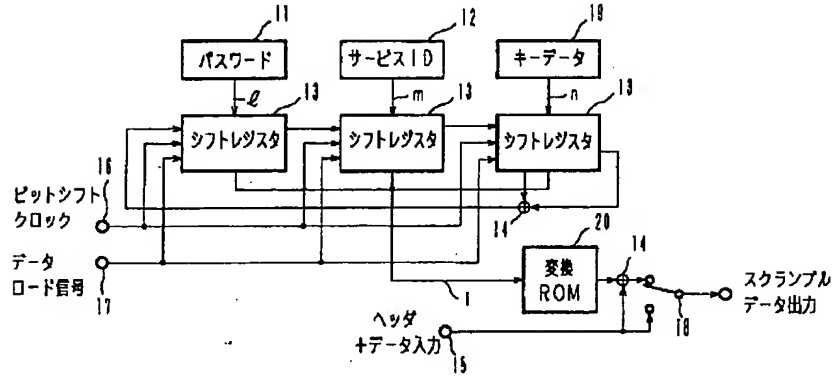
7　　8

１３　シフトレジスタ
１４　排他的論理和回路
１５　データ入力端子
１６　ビットシフトクロック入力端子
１７　データロード信号入力端子
２０　データ変換ＲＯＭ

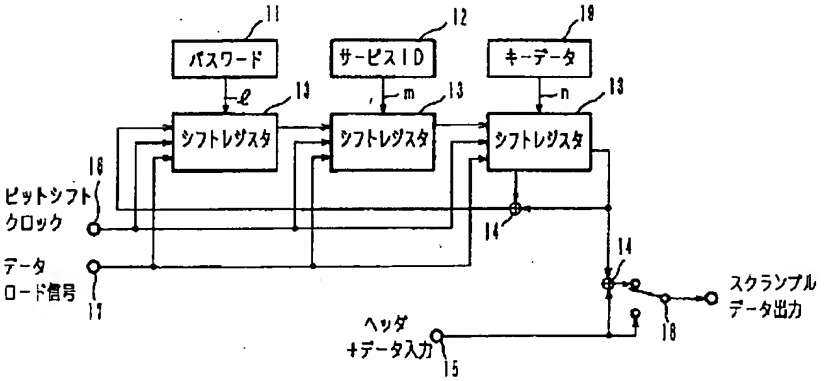
【図１】



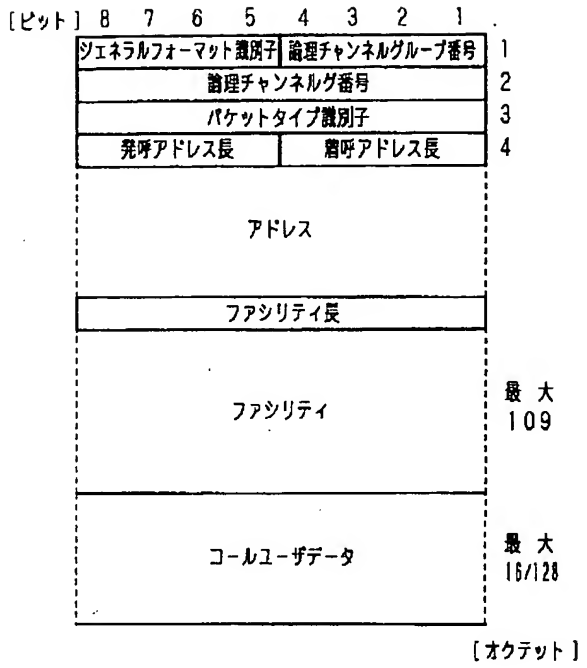
【図２】



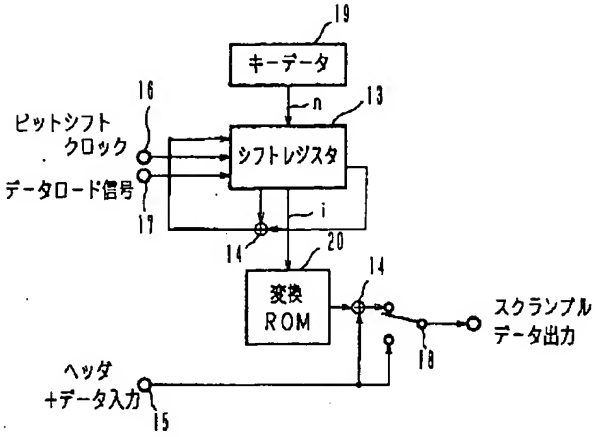
【図３】



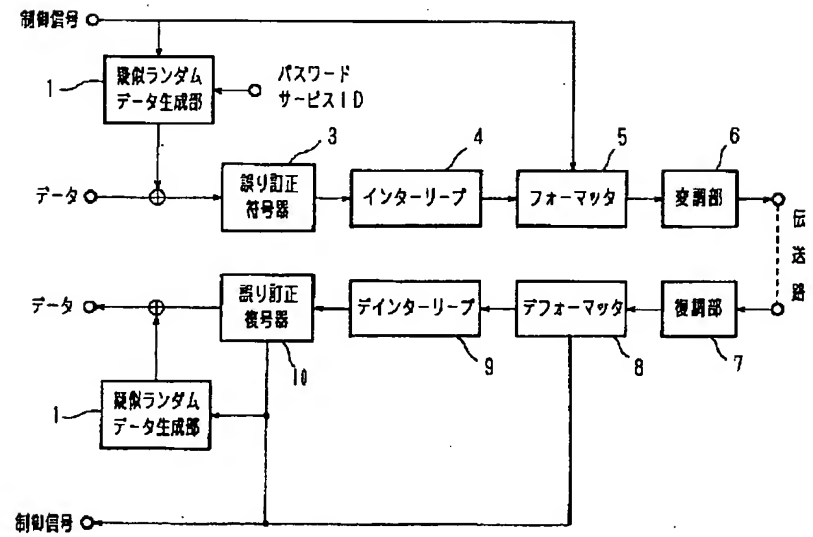
【図4】



【図6】

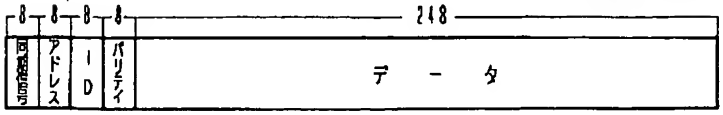


【図5】

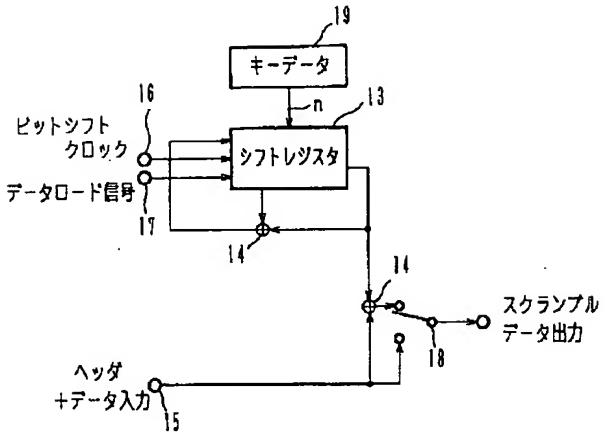


【図9】

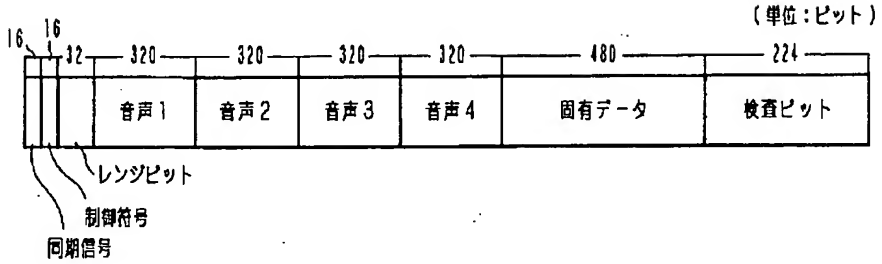
（単位：ビット）



【図7】



【図8】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI	技術表示箇所
G11B 20/10		F 7923－5D		